By Lana K. Varney and Oliver P. Thoma

Defending Your Client's Confidential Documents in the Big Data Age

When elections and economies depend on protecting the integrity of data, it should not be surprising to see bad actors threatening the integrity of such data. Facebook's recent data privacy scandal has reminded the public that we live in the age of "big data" where mass volumes of data are collected, sifted, and analyzed until trends or patterns emerge. As technology advances, more and more data will be collected to be commoditized and sold to the highest bidder.

There is a corollary here that lawyers should be careful to observe. In the e-discovery age in which we find ourselves, the production of massive volumes of electronically stored information (ESI) is increasingly common in civil litigation or government investigations. Data produced in discovery routinely contains sensitive commercial information that could have negative economic consequences if it is publically disseminated. Beyond pure trade secrets (*e.g.*, the Coca-Cola formula), there are vast volumes of "customer relationship management" (*i.e.*, "CRM") data that can be mined by direct economic competitors if it is produced without adequate protection.

Moreover, the plaintiffs' bar has achieved an unprecedented level of coordination,

■ Lana K. Varney is a partner and Oliver P. Thoma is an associate of King & Spalding LLP in Austin, Texas. Ms. Varney has held several lead counsel roles representing international and national pharmaceutical and medical device companies in product liability litigation across the United States. Mr. Thoma represents companies in the life sciences and health-care sectors in high-profile product liability and mass tort litigation. Both authors are members of DRI and its Drug and Medical Device Committee.

especially in the recent wave of mass torts and multidistrict litigations (MDLs). Today we routinely see the plaintiffs' bar use mass tort discovery to (1) create "discovery in a box" to sell to the next plaintiffs' firm; (2) use as leverage on defendants to settle; and (3) post on social media sites for reasons ranging from informing the public to drumming up more cases.

These present realities make it increasingly important that in-house counsel ask their outside counsel how their data is being protected. The first place to start is getting a discovery protective order entered in each case before any documents are produced.

A Brief History of Discovery Protective Orders

Discovery protective orders are generally limited to a single case and prevent the dissemination of information or documents obtained during discovery to that particular case. The exception to this rule is where a discovery protective order is entered as to an entire MDL, and the plaintiffs' steering committee is tasked with pursuing common discovery to share with other plaintiffs' firms in exchange for reimbursement from a common benefit fund. However, even an MDL discovery protective order typically limits discovery sharing to plaintiffs' firms with filed cases in the MDL, and only for their filed MDL cases.

The inherent authority granted to trial courts has always included the ability to protect certain categories of sensitive commercial information. This practice was generally supported by case law and various rules of civil procedure, but it was frequently limited to trade secrets.

However, in 1970, the Federal Rules of Civil Procedure broadened the protection to include "other confidential commercial information" to reflect a growing trend in the case law. Fed R. Civ. P. 26(c)(1), (c)(1)(G), and advisory comm.'s notes to 1970 amendment ("The court may, for good cause, issue an order to protect a party or person from… requiring that a *trade secret or other confidential research, development, or commercial information* not be revealed or be revealed only in a specified way.") (emphasis added).

In 1979, the Supreme Court of the United States affirmed Rule 26(c)'s broad view of confidential information by opining that certain governmental records were confidential commercial information, even though such records were not trade secrets and would eventually become public record. *Fed. Open Mkt. Comm. of Fed. Reserve Sys. v. Merrill*, 443 U.S. 340, 356–57, 361–63 (1979) (citing Fed. R. Civ. P. 26(c)(7), now codified as 26(c)(1)(G)). The *Merrill* Court remanded the case noting that a Rule 26(c) protective order limiting the dissemination of such government records would not be a violation of the Freedom of Information Act (FOIA). The *Merrill* Court recognized that it was common, accepted practice for a trial court to enter a protective order restricting disclosure of discovery to counsel under Rule 26(c). *Id.* at 362 n.24.

The inherent authority granted to trial courts has always included the ability to protect certain categories of sensitive commercial information. This practice was generally supported by case law and various rules of civil procedure, but it was frequently limited to trade secrets.

More recently, the Ninth Circuit reaffirmed the open-ended language used in Rule 26(c): "The law, however, gives district courts broad latitude to grant protective orders to prevent disclosure of materials for many types of information, including, *but not limited to*, trade secrets or other confidential research, development, or commercial information." *Phillips ex rel. Estates of Byrd v. Gen. Motors Corp.*, 307 F.3d 1206, 1211 (9th Cir. 2002) (citing Fed. R. 26(c)) (emphasis in original). The Ninth Circuit reinforced the proposition that protective orders are not limited to trade secrets or even "other confidential research, development, or commercial information." *See generally* 8A Charles Alan Wright & Arthur R. Miller, Fed. Prac. & Proc. Civ. §2043 (3d ed. 2008). Thus, protective orders can broadly apply to nonpublic information that would not merit trade secret protection but that the disclosure of which would be potentially damaging to your company.

Plaintiffs' Frequent Line of Attack: Presumptive Right of Public Access

The plaintiffs' bar has traditionally challenged protective orders under the pretext of "the public's right to know." However, there is no presumptive right of public access to *all* discovery under the Federal Rules of Civil Procedure. This was reinforced after the 2000 amendment to Federal Rule of Civil Procedure 5(d), because parties were no longer required to file discovery with the court. Thus, there is no presumptive right of public access to *unfiled discovery* in federal court. *See Bond v. Utreras*, 585 F.3d 1061, 1075–76 (7th Cir. 2009); *SEC v. TheStreet.com*, 273 F.3d 222, 233 n.11 (2d Cir. 2001). The "presumptive right of public access" is much narrower in scope and only applies to what is filed with the court. Correspondingly, the Supreme Court has held that parties' First Amendment rights are not violated under a Rule 26(c) protective order or state court equivalent limiting the dissemination of documents obtained in pretrial civil discovery. *See Seattle Times Co. v. Rhinehart*, 467 U.S. 20, 37 (1984).

Instructive on this topic is the 1984 Supreme Court case *Seattle Times Co. v. Rhinehart*. In *Rhinehart*, the Supreme Court upheld a Washington state court protective order limiting the dissemination of information obtained during pretrial discovery. In reaching its opinion, the *Rhinehart* Court observed that pretrial discovery was not open to the public at common law. *Id.* at 33. The Court further noted that much of the information obtained during pretrial discovery is only tangen-

tially related to the underlying cause of action. *Id.*

Accordingly, the *Rhinehart* Court identified the potential abuse that could result from eliminating protective orders: the use of civil discovery as a *Trojan horse* to acquire confidential information that is not applicable to the merits of the case at hand that could be "damaging to reputation or privacy" if publically disseminated. *Id.* at 35. The Court went on to hold that "[t]he prevention of the abuse that can attend the coerced production of information under a State's discovery rule is sufficient justification for the authorization of protective orders." *Id* at 35–36.

Despite the *Rhinehart* decision and the 2000 amendment to Rule 5(d), the plaintiffs' bar has succeeded in perpetuating the idea that a presumptive right of public access extends to *all* discovery. And in a few states, such as Texas and Florida, the plaintiffs' bar has succeeded in passing complex, time-consuming, motion-intense legislation, which has broad definitions of what should be subject to public access. *See* Tex. R. Civ. P. 76a (defining "court records" to include unfiled discovery "concerning matters that have a probable adverse effect upon the general public health or safety, or the administration of public office, or the operation of government."). *See also* Fla. Stat. §69.081 ("[N]o court shall enter an order or judgment which has the purpose or effect of concealing a public hazard or any information concerning a public hazard….").

One scholar has suggested that this line of attack survives in large part because the media has also realized that such a position is advantageous: "they want discovery to become an equivalent of the Freedom of Information Act so that they can mine it as a source for stories they want to present." Richard L. Marcus, *A Modest Proposal: Recognizing (at Last) That the Federal Rules Do Not Declare That Discovery Is Presumptively Public*, 81 Chi.-Kent L. Rev. 331, 351 (2006). Nevertheless, federal courts have continued to reject the idea and have held that "[i]t is a mistake to conclude… that Rule 26(c) creates a freestanding public right of access to unfiled discovery." *Bond*, 585 F.3d at 1076 (Seventh Circuit); *SEC v. TheStreet.com*, 273 F.3d at 233 n.11 (Second Circuit); *Chicago Tribune Co. v. Bridgestone/Firestone, Inc.*, 263 F.3d 1304, 1313n.10 (11th Cir. 2001) (Eleventh Circuit).

Regardless of the reason, the plaintiffs' bar is looking for ways to share your company's confidential information, and you must be prepared to stop it.

Define who will have access to information designated as "confidential." For instance, consider a provision that prevents disclosure of produced documents to a "consultant to a competitor" absent prior notice and an opportunity for the producing party to seek a ruling from the court.

Setting Yourself up for Success

Here are some tips for maximizing the success of your agreed, discovery protective order.

First, carefully define what is considered "confidential" so that it is broader than just trade secrets. For instance, counsel involved in litigation involving an industry or product that is regulated by a government authority should include references to confidentiality as it is used in regulations promulgated by the regulating authority.

In the recent female pelvic mesh MDLs, each of the MDLs has a discovery protective order that defines "confidential" information to include "materials that are deemed confidential under Federal Drug Administration ('FDA') regulations and Health Insurance Portability and Accountability Act ('HIPAA') statutes and/or regulations."

Second, define who will have access to information designated as "confidential." For instance, consider a provision that prevents disclosure of produced documents to a "consultant to a competitor" absent prior notice and an opportunity for the producing party to seek a ruling from the court. This generally occurs with testifying or consulting experts hired by the opposing party. This gives your company an opportunity to gauge whether your corporate competitors may be trying to use discovery as a *Trojan horse* to obtain confidential commercial information.

Third, list the procedural steps and legal standard for challenging the designation of information as "confidential." Make sure that your protective order accurately reflects your jurisdiction's views on the standard for prevailing on protective orders or filing documents in camera or under seal.

When motions are filed to challenge the protective order or particular documents, be sure that you or your opposing counsel do not file "confidential" documents on the public docket. Rather, be sure to file such documents in camera or under seal, depending upon your jurisdiction's conventions.

Fourth, require a party challenging a document's confidentiality to meet and confer before filing any related motion to give an opportunity to the designating party to de-designate or partially redact a challenged document if it is possible to do so.

The Opioid MDL in the Northern District of Ohio required a similar provision in its discovery protective order governing the confidentiality of documents produced by the Drug Enforcement Agency: "Before filing any motions or objections to a confidentiality designation with the Court, the objecting party shall have an obligation to meet and confer in a good faith effort to resolve the objection by agreement." *In re: National Prescription Opiate Litigation*, MDL No. 2804, Dkt. #167, ¶11 (March 6, 2018).

Fifth, require a party challenging confidentiality to list specific Bates ranges to avoid general challenges to the entire protective order.

Sixth, ensure that motions challenging the confidentiality order cannot be filed without first seeking a briefing sched-

ule from the court to allow sufficient time for you to gather supporting affidavits and other evidence in support of your defense of confidentiality (*e.g.*, 45 days).

Finally, define how "confidential" information should be disposed of after the case is resolved. Specify whether the plaintiff's counsel must destroy or return the produced documents. Be sure to specify the length of time that the plaintiff's counsel has to comply with destroying or returning the produced documents, and make that time as short as possible. Make sure that you get written confirmation from your opposing counsel on compliance with this provision. Consider making opposing counsel's written confirmation of destruction or return of the documents a *condition precedent* to distribution of proceeds paid under any settlement agreement.

Protecting Your Agreed, Discovery Protective Order

Even well-written, agreed-to discovery protective orders are subject to challenge given the right motivation by opposing counsel. Be prepared for motion practice by considering the basic requirements to prevail on a challenge to your protective order, or the confidentiality of a particular document.

Generally, you must show good cause pertaining to why your company's information is, in fact, a trade secret or another type of protected, confidential information covered by the protective order and that some harm would befall your company if the information was not protected from public dissemination.

Such a showing requires specificity, and best practice dictates acquiring affidavits from company employees who can attest to the steps the company has taken to keep the information confidential as well as the commercial harm that might occur if such information was publicly disclosed. Such affidavits can be written to address categories of documents rather than each individual document, unless your jurisdiction requires otherwise.

You should show the court your *reliance* on the discovery protective order—that is, that you produced documents to the plaintiff's counsel in reliance on the order, rather than fight on each and every confidential document prior to production.

Courts do not take kindly to plaintiffs' counsel who engage in a bait-and-switch: "Indeed, the phrase 'protective order' becomes a misnomer if parties are unable to trust them—or trust the courts that enforce them—thus fueling litigation that is far more contentious and far more expensive." *In re Ford Motor Co.*, 211 S.W.3d 295, 301 (Tex. 2006). *See also* Arthur R. Miller, *Confidentiality, Protective Orders, and Public Access to the Courts*, 105 Harv. L. Rev. 427, 501 (1991) ("The reality seems obvious: for protective orders to be effective, litigants must be able to rely on them.").

Preparing for the Future

As technology advances and analyzing large volumes of electronic data becomes quicker and less expensive, defense counsel should be prepared for a plaintiffs' bar that can quickly mine large document productions for key documents and company histories on a particular litigation issue. Technology already exists to analyze and create captivating visualizations of relationships between company employees on a particular topic. Such visualizations help create a narrative from big data that can be used in everything from litigation strategy to persuading a jury at trial. Likewise, such information can be mined by your company's competitors. Consequently, it is imperative to protect your company's data adequately during discovery. Do not forget to start with a well-crafted discovery protective order.